Smirnov Alexey, Doctor of technical sciences, Associate Professor, Professor of Academic Department of software Kirovograd National Technical University.

Дрейс Юрий Александрович, кандидат технических наук, доцент кафедры безопасности информационных и коммуникационных систем Житомирского военного института им. С.П. Королева Государственного университета телекоммуникаций.
E-mail: dr_yr_al@mail.ru
Дрейс Юрій Олександрович, кандидат технічних наук, доцент кафедри безпеки інформаційних і комунікаційних систем Житомирського військового інституту ім. С.П. Корольова Державного університету телекомунікацій.

Dreis Yurii, PhD in Eng., Associate Professor of Academic Department of Security Information and Communication Systems of the Zhytomyr Military Institute named after S.P. Koroleva of the State University of Telecommunication.

Даниленко Дмитрий Алексеевич, аспирант кафедры программного обеспечения Кировоградского национального технического университета.
E-mail: dmitriy.danilenko@kiroe.com.ua
Даниленко Дмитро Олексійович, аспірант кафедри програмного забезпечення Кіровоградського національного технічного університету.
Danilenko Dmitry, graduate student of Academic Department of software Kirovograd National Technical University.

УДК 004.056.5(045)

РІШЕННЯ ЗВОРОТНОЇ ЗАДАЧІ ЕКОНОМІЧНОГО МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Євген Левченко, Руслана Прус

При розв'язку зворотної задачі економічного менеджменту задають параметри інформаційної системи і знаходять необхідну кількість ресурсів і їх оптимальний розподіл між об'єктами. Критерієм оптимальності є мінімізація загальних втрат, які включають втрати від витоку інформації і витрати на її захист, або максимізація прибутку від інвестицій в захист і їх рентабельності. Розглянуто систему з двох об'єктів, які відрізняються вразливістю і кількістю інформації. Розв'язок знаходиться в області існування сідлової точки, що забезпечує реальність одержаних результатів, оскільки ні одна з сторін не зацікавлена в зміні своєї стратегії. Виконання обох умов – забезпечення режиму сідлової точки і оптимізація розподілу ресурсів – досягається шляхом управління параметрами інформаційної системи – вразливостями об'єктів і розподілом інформації по об'єктах. Рішення зворотної задачі є першим кроком до синтезу системи. Наступний крок – вибір засобів захисту для кожного об'єкта з врахуванням їх вартості та імовірності нейтралізації можливих загроз.

Ключові слова: *інформаційна безпека, математична модель, вразливість, оптимізація, сідлова точка.*

Вступ. Розвиток інформаційної сфери приводить до зростання обсягів і вартості інформації і, як наслідок, до ускладнення систем захисту та збільшення їх вартості. В цих умовах зростають вимоги до створення систем, в яких досягаються найкращі технічні та економічні показники.

Рішення поставленої задачі утруднене через низку причин. Це складність багаторівневих багаторубіжних систем захисту, невизначеність дій суперника, неможливість точного визначення захисних спроможностей системи, зокрема, такого важливого показника, як її вразливість, а також відсутність статистичної інформації про результати протистояння систем нападу і захисту. Через ці складнощі основна увага при дослідженні захисних систем приділяється їх аналізу, хоча створення оптимальних систем часто несе в собі елементи синтезу.

Аналіз системи захисту може вестись в двох протилежних напрямках:

– пряма задача – по заданим ресурсам захисту визначити частку втраченої інформації;

– зворотна задача – по заданому граничному значенню втрат інформації визначити необхідну кількість ресурсів захисту.

Рішення зворотної задачі складніше, ніж прямої, проте ця задача викликає значний інтерес, оскільки її розв'язок можна вважати першим кроком у синтезі оптимальних систем захисту.

Мета роботи – розробка методики розв'язку зворотної задачі, який забезпечує досягнення оптимальних значень показників інформаційної системи.

Постановка задачі. Використаємо математичну модель [1], відповідно до якої цільова функція $i(x,y)$ виражає частку загальних втрат інформації і для однорівневої системи має вигляд:

$$i(x,y)=\sum_{k=1}^{l} i_k(x_k,y_k)=\sum_{k=1}^{l} g_k p_k q_k(x_k,y_k) f_k(x_k,y_k), \quad (1)$$

де x і y – ресурси нападу і, відповідно, захисту, $\sum_{k=1}^{l} x_k = X$, $\sum_{k=1}^{l} y_k = Y$; $k=\overline{1,l}$ – номер об'єкта; g_k – відносна вартість інформації на k-му об'єкті, $\sum_{k=1}^{l} g_k = 1$; p_k – імовірність нападу на k-й об'єкт; $q_k(x,y)$ – щільність двовимірного розподілу імовірності виділення сторонами ресурсів x і y на k-й об'єкт; $f_k(x,y)$ – частка втраченої інформації на k-му об'єкті, що виражає вразливість об'єкта.

Величини $i(x,y)$, X, Y віднесені до загальної вартості інформації, $i_k(x,y)$, $f_k(x,y)$, g_k – до вартості інформації на об'єкті.

На першому етапі зосередимось на впливі величин g_k, $f_k(x,y)$. З цією метою покладемо $p_k=1$, $q_k(x,y)=const=1$ в інтервалі значень x, y, які ми будемо розглядати.

Розглянемо структуру (рис. 1), де зображено: g_1, g_2 – об'єкти захисту, які містять відповідну частку загальної інформації; f_1, f_2 – захисні перешкоди, які виражають вразливості об'єктів g_1, g_2; X, Y – загальна кількість ресурсів нападу і, відповідно, захисту; x_1, x_2 та y_1, y_2 – ресурси нападу і, відповідно, захисту, направлені на об'єкти g_1, g_2.

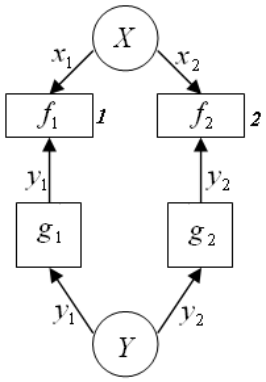

Рис. 1. Схема інформаційного протистояння

Для структури (рис. 1) цільова функція має вигляд:

$$i(x,y)=i_1(x_1,y_1)+i_2(x_2,y_2)=g_1 f_1(x_1,y_1)+g_2 f_2(x_2,y_2). \quad (2)$$

При виборі форми функцій $f(x,y)$ враховано наступні міркування [1]: змінні x і y входять у ці функції у вигляді відношення x/y, тобто вразливості залежать від співвідношення ресурсів нападу і захисту на даному елементі. Крім того, з фізичних міркувань випливає, що при $x/y \to 0$ $f(x,y)\to 0$, а при $x/y \to \infty$ $f(x,y)\to 1$. Цим умовам задовольняють функції виду:

$$f(x,y)=\frac{\left(x/y\right)^n}{\left(x/y\right)^n + c}. \quad (3)$$

При формулюванні задачі задається тип об'єктів (фізичні, електронні – цим визначається форма функцій вразливості, тобто значення параметрів n, c в (3)) і критерій оптимуму системи. В подальшому можливі різні варіанти постановки задачі:

1. Задається граничний рівень втрат і визначається необхідна кількість ресурсів захисту Y за умови їх оптимального розподілу $\{y_k^0\}$ між об'єктами.

2. Задається мінімальний рівень сумарних втрат, які включають ресурси, виділені на захист, і втрати від витоку інформації, і визначається необхідна кількість ресурсів захисту.

3. Задаються типи загроз та імовірності їх реалізації, можливі засоби захисту, а також імовірності нейтралізації окремих загроз кожним із засобів та їх вартість; визначається оптимальний набір засобів для кожного з об'єктів системи, який гарантує мінімальні загальні втрати інформації при заданих обмеженнях на кількість ресурсів захисту.

Щодо параметрів розрахунку, а саме вразливостей і розподілу інформації по об'єктах, то можливі два обернених варіанта:

– задано $\{g_k\}$, знаходимо $\{f_k\}$;

– задано $\{f_k\}$, знаходимо $\{g_k\}$.

Інформаційне протистояння відбувається в умовах невизначеності, коли наміри суперника невідомі і можуть бути визначені лише з певною імовірністю. При використанні обраної моделі невизначеність торкається кількості X ресурсів нападу і їх розподілу між об'єктами $\{x_k\}$. В цих умовах доводиться розглядати всі варіанти можливих значень. Проте є один варіант розподілу

ресурсів $\{x_k^0\}$, $\{y_k^0\}$, який є прийнятним для обох сторін. Цей варіант в термінології теорії ігор відомий як рівновага за Нешем [2], а при графічному представленні протистояння зображується сідловою точкою [3]. Відхилення від прийнятих розподілів в цій точці веде до небажаного результату для кожної з сторін: збільшення $i(x,y)$ при відхиленні від розподілу $\{y_k^0\}$ і зменшенні $i(x,y)$ при відхиленні від розподілу $\{x_k^0\}$.

Відповідно до [4, 5], сідлова точка існує в певному інтервалі значень $Z=\frac{X}{Y}$, ширина якого ΔZ залежить від структури системи захисту, форми протистояння, форми функцій $f_k(x,y)$ і розподілу $\{g_k\}$.. В наших розрахунках пошук рішення ведеться за умови, що це рішення відповідає сідловій точці.

Результати досліджень. Розрахунки проведено для структури (рис. 1) при двох варіантах постановки задачі.

1. Використовується перша постановка задачі. Операції виконуються в такій послідовності.

– Відомим вважаємо граничний рівень втрат i_m і кількість ресурсів нападу X.

– Задано вразливості об'єктів, тобто параметри n_k, c_k, та розподіл $\{g_k\}$ інформації по об'єктах.

– Виходячи з заданих величин, визначаємо інтервал ΔZ існування сідлової точки.

– З інтервалу ΔZ знаходимо мінімально можливу кількість ресурсів захисту Y, для якої виконується умова $i(x,y)\le i_m$ при оптимальному розподілі $\{y_k^0\}$ ресурсів захисту по об'єктах.

– Фіксуємо результат: вразливості $f_k(x,y)$ елементів схеми, розподіл $\{g_k\}$ інформації по об'єктах, кількість ресурсів нападу X і захисту Y, розподіл $\{y_k^0\}$ ресурсів захисту по об'єктах.

– Якщо сідлова точка при заданих умовах не існує ($\Delta Z=0$), то слід змінити форму функцій $f_k(x,y)$ або розподіл $\{g_k\}$ (або те й інше) і повторити описані операції до отримання кінцевого результату.

Результати розрахунків зображені на рис. 2. Вибір розрахункових параметрів пояснюється наступними причинами. Одна з функцій вразливостей $f_k(x,y)$ обрана нелінійною ($n_1=2$), оскільки в системі з двох об'єктів при обох дробово-лінійних функціях інтервал ΔZ існування сідлової точки необмежений [4]. Розподіл $\{g_k\}$ інформації по об'єктах визначається співвідношенням між вразливостями: на об'єкті з більшою вразливістю ($n_1>n_2$) зосереджена менша частина інформації ($g_1<g_2$). Вибір коефіцієнтів c_k забезпечує розташування робочої точки А, де $i(Z)$ відповідає заданому значенню $i_m=0,23$, поблизу нижньої границі інтервалу ΔZ.

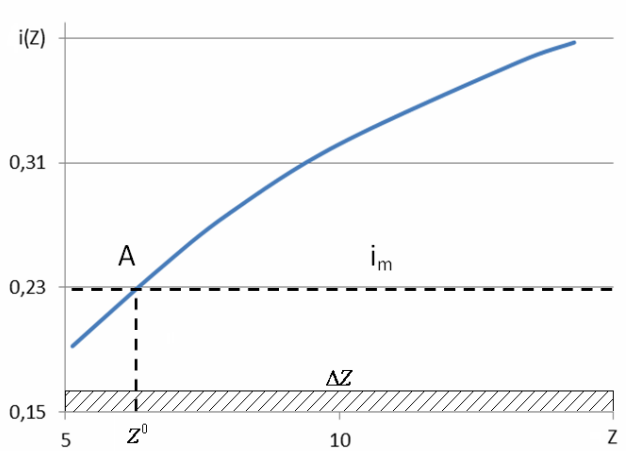

Рис. 2. Залежність втрат інформації від співвідношення ресурсів нападу і захисту в інтервалі існування сідлової точки при значеннях параметрів: $g_1=0,3$, $g_2=0,7$, $n_1=2$, $n_2=1$, $c_1=32$, $c_2=64$

Точне співпадіння точки А з нижньою границею недоцільне, оскільки не забезпечує надійного виконання умови про режим сідлової точки. Значення X в розрахунках прийнято рівним $X=2$. З визначеної величини $Z^0=6,35$ знаходимо $Y^0=0,315$. Оптимальний розподіл ресурсів захисту по об'єктах: $y_1^0=0,227$, $y_2^0=0,088$. В даному розрахунку розподіл інформації $\{g_k\}$ по об'єктах визначається вразливостями об'єктів, тобто заданою формою функцій $f_k(x,y)$.

2. Друга постановка задачі. Результати зображені на рис. 3.

Функції вразливості обрані дробово-лінійними ($n_1=n_2=1$), оскільки при дробово-нелінійних функціях $f_k(x,y)$ оптимум Y^0 залежності $S(y)$, що відповідає мінімальному значенню $S(y)$, знаходиться за межами реальних величин Y. Мінімум сумарних втрат $S(Y^0)$ відповідає максимуму прибутку $b(Y^0)$. Кількість захищеної інформації $j(Y)$ після досягнення оптимальної точки продовжує зростати, але з меншою швидкістю.

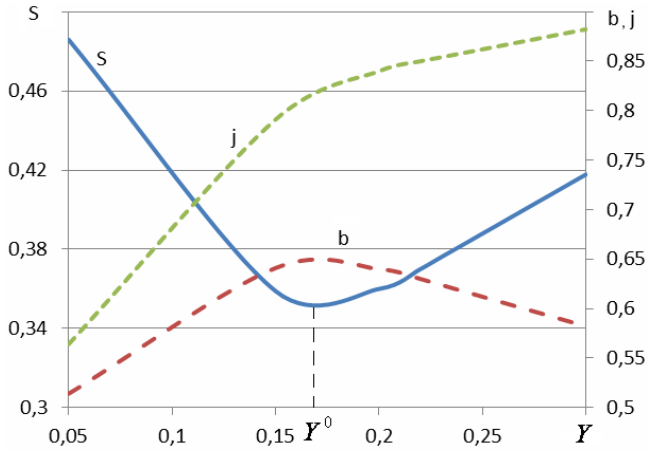

Рис. 3. Залежність сумарних втрат $S(Y)$, прибутку $b(Y)$, частки захищеної інформації $j(Y)$ від інвестицій в захист при $g_1 = 0{,}3$, $g_2 = 0{,}7$, $n_1 = n_2 = 1$, $c_1 = 16$, $c_2 = 32$

Висновки. Проведені розрахунки дозволяють зробити деякі попередні висновки.

При створенні ефективної системи захисту повинні бути визначені наступні величини:

– форма функцій вразливості $f_k(x, y)$, тобто значення параметрів n і c;

– розподіл інформації $\{g_k\}$ по об'єктах;

– мінімальна необхідна кількість ресурсів Y захисту (за умови їх оптимального розподілу $\{y_k^0\}$).

Кількість втраченої інформації залежить від трьох зазначених величин. Отже, існує три ступені свободи, які впливають на величину $i(x, y)$. Звичайно, можливі ситуації, коли деякі з цих величин, наприклад, кількість ресурсів захисту або розподіл $\{g_k\}$ – задані заздалегідь. В цьому випадку задача спрощується, проте, залишаються труднощі, пов'язані з невизначеністю дій суперника, зокрема, з величиною виділених ресурсів X нападу і їх розподілом $\{x_k\}$ по об'єктах. В цих умовах величину X будемо задавати, вважаючи її обмеженою деяким значенням, а розподіл ресурсів буде визначеним для обох сторін, якщо протистояння відбувається в сідловій точці цільової функції.

ЛІТЕРАТУРА

[1]. Левченко Є.Г. Оптимізаційні задачі менеджменту інформаційної безпеки / Є.Г. Левченко, А.О. Рабчун // Сучасний захист інформації. – 2010. – №1. – С. 16-23.

[2]. Вэриан Х. Микроэкономика / Х. Вэриан. – М.: Юнити, 1977. – 767 с.

[3]. Шикин Е.В. Исследование операций / Е.В. Шикин, Г.Е. Шикина. – М.: Проспект, 2006. – 280 с.

[4]. Левченко Є.Г. Умови існування сідлової точки в багаторубіжних системах захисту інформації / Є.Г. Левченкко, Р.Б. Прус, Д.І. Рабчун // Безпека інформації. – 2013. – №1. – С. 70-76.

[5]. Левченко Є.Г. Вплив форми протистояння на оптимізацію процесу управління ресурсами захисту інформації / Є.Г. Левченкко, Р.Б. Прус, Д.І. Рабчун // Безпека інформації. – 2013. – Том 19, №3. – С. 70-76.

REFERENCES

[1]. Levchenko E., Rabchun A. (2010) "Optimization problems of Information Security Management", Modern Information Security, №1, pp. 16-23.

[2]. Varian H. (1977) "Microeconomics", M.: Unity, 767 p.

[3]. Shikin E., Shikina G. (2006) "Operation Research", M.: Prosrect, 280 p.

[4]. Levchenko E., Prus R., Rabchun D. (2013) "Conditions of saddle point existence in multilevel information security systems", Information Security, №1, pp. 70-76.

[5]. Levchenko E., Prus R., Rabchun D. (2013) "Influence of confrontation form on optimization of information security resource allocation process", Information Security, №3, pp. 218-223.

РЕШЕНИЕ ОБРАТНОЙ ЗАДАЧИ ЭКОНОМИЧЕСКОГО МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

При решении обратной задачи экономического менеджмента задают параметры информационной системы и находят необходимое количество ресурсов и их оптимальное распределение между объектами. Критерием оптимальности выступает минимизация общих потерь, которые включают потери от утечки информации и затраты на ее защиту, или максимизация прибыли от инвестиций в защиту и их рентабельности. Рассмотрено систему из двух объектов, которые отличаются уязвимостью и количеством информации. Решение находится в области существования седловой точки, что обеспечивает реальность полученных результатов, поскольку ни одна из сторон не заинтересована в изменении своей стратегии. Выполнение обеих условий – обеспечение режима седловой точки и оптимизация распределения ресурсов – достигается путем управления параметрами информационной системы: уязвимостями объектов и распределением информации по объектам. Решение обратной задачи – первый шаг к синтезу системы. Следующий шаг – выбор средств защиты для каждого объекта с учетом их стоимости и вероятности нейтрализации возможных угроз.

Ключевые слова: информационная безопасность, математическая модель, уязвимость, оптимизация, седловая точка.

SOLUTION TO THE INVERSE PROBLEM OF INFORMATION SECURITY ECONOMIC MANAGEMENT

For finding solution to the inverse problem of economic management parameters of information system must be specified and required resource amount and optimal resource allocation between objects must be found. Criterion of optimality is minimization of total loss, which includes loss from information leakage and security costs, or maximization of security investment benefit and its profitability. System of two objects is considered; objects are differed in vulnerability and information quantity. Solution is found in area of saddle point existence, what provides reality of findings, since neither of sides interested in changing their strategy. Fulfilling both conditions – guaranteeing of saddle point state and optimization of resource allocation – is achieved by controlling of information system parameters: object vulnerabilities and information distribution between the objects. The solution to the inverse problem is the first step to system synthesis. Next step is choosing security mechanisms for each object with a glance of their price and threat neutralizing probabilities.

Keywords: information security, mathematical model, vulnerability, optimization, saddle point.

Левченко Євген Григорович, кандидат фізико-математичних наук, доцент кафедри засобів захисту інформації Національного авіаційного університету.
E-mail: ruslana_prus@meta.ua
Левченко Евгений Григорьевич, кандидат физико-математических наук, доцент кафедры средств защиты информации Национального авиационного университета.
Levchenko Evgen, PhD in Physics and Math, Associate Professor of Information Security Equipment Department, National Aviation University (Kyiv, Ukraine).

Прус Руслана Богданівна, аспірант кафедри засобів захисту інформації Національного авіаційного університету.
E-mail: ruslana_prus@meta.ua
Прус Руслана Богдановна, аспирант кафедры средств защиты информации Национального авиационного университета.
Prus Ruslana, postgraduate student Academic Department of Information Security Means, National Aviation University (Kyiv, Ukraine).

УДК 004.056.53

БЕЗОПАСНОСТЬ ПОЛЬЗОВАТЕЛЬСКИХ ПРОЦЕДУР АУТЕНТИФИКАЦИИ WEB-ПРИЛОЖЕНИЙ

Михаил Коломыцев, Светлана Носок, Николай Грайворонский

Интерактивные Web-приложения в настоящее время являются важной частью информационных систем самого разного назначения – бизнеса, государственных структур и других. Основной особенностью таких систем является организация доступа клиентов, деловых партнеров и собственных сотрудников к информационным ресурсам через Интернет. Для доступа к онлайн-услугам, определения уровня полномочий, пользователи должны однозначно идентифицировать себя. Существует множество способов организации процесса аутентификации пользователей, из которых чаще всего используется аутентификация с помощью форм. В статье рассматриваются рекомендации, направленные на повышение безопасности процесса аутентификации и управления сессиями пользователей.
Ключевые слова: *Web-приложения, аутентификация, атака, процес аутентификации, информационная система.*

Вступление. Целью статьи – дать рекомендации разработчикам по повышению безопасности WEB-приложений.

Интерактивные Web-приложения в настоящее время являются важной частью информационных систем самого разного назначения – бизнеса, государственных структур и других. Основной особенностью таких систем является организация доступа клиентов, деловых партнеров и собственных сотрудников к ресурсам системы через Интернет. Для доступа к онлайн-услугам, определения уровня полномочий, пользователи должны однозначно идентифицировать себя. Существует множество способов организации процесса аутентификации пользователей [1,3], из которых чаще всего используется аутентификация с помощью форм [2]. Разработчики понимают важность корректной реализации механизма аутентификации, однако использование собственных разработок для реализации этого механизма зачастую приводит к возникновению уязвимостей. В статье рассматриваются вопросы, связанные с повышением безопасности процесса аутентификации и управления сессиями пользователей.

Встроенные в протокол HTTP схемы аутентификации пригодны для использования [5], особенно если устанавливается защищенное соединение по протоколу SSL. Однако разработчи-